Ad Hoc Networks 36 (2016) 152–176

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment

Mohammad Sabzinejad Farash[a], Muhamed Turkanović[b], Saru Kumari[c], Marko Hölbl[b,*]

[a] Faculty of Mathematical Sciences and Computer, Kharazmi University, P.O. Box 15719-14911, Tehran, Iran
[b] University of Maribor, Faculty of Electrical Engineering and Computer Science, 2000 Maribor, Slovenia
[c] Department of Mathematics, Ch. Charan Singh University, Meerut 250005, Uttar Pradesh, India

ARTICLE INFO

Article history:
Received 8 November 2014
Revised 20 April 2015
Accepted 27 May 2015
Available online 10 June 2015

Keywords:
Internet of Things
Wireless sensor networks
Key agreement
Authentication
BAN-logic
AVISPA tools

ABSTRACT

The concept of Internet of Things (IOT), which is already at our front doors, is that every object in the Internet infrastructure (II) is interconnected into a global dynamic expanding network. Sensors and smart objects are beside classical computing devices key parties of the IOT. We can already exploit the benefits of the IOT by using various weareables or smart phones which are full of diverse sensors and actuators and are connected to the II via GPRS or Wi-Fi. Since sensors are a key part of IOT, thus are wireless sensor networks (WSN). Researchers are already working on new techniques and efficient approaches on how to integrate WSN better into the IOT environment. One aspect of it is the security aspect of the integration. Recently, Turkanović et al.'s proposed a highly efficient and novel user authentication and key agreement scheme (UAKAS) for heterogeneous WSN (HWSN) which was adapted to the IOT notion. Their scheme presented a novel approach where a user from the IOT can authenticate with a specific sensor node from the HWSN without having to communicate with a gateway node. Moreover their scheme is highly efficient since it is based on a simple symmetric cryptosystem. Unfortunately we have found that Turkanović et al.'s scheme has some security shortcomings and is susceptible to some cryptographic attacks. This paper focuses on overcoming the security weaknesses of Turkanović et al.'s scheme, by proposing a new and improved UAKAS. The proposed scheme enables the same functionality but improves the security level and enables the HWSN to dynamically grow without influencing any party involved in the UAKAS. The results of security analysis by BAN-logic and AVISPA tools confirm the security properties of the proposed scheme.

1. Introduction

Wireless Sensor Networks (WSN) are crucial for the future of Internet of Things (IOT) since they cover a wide application range essential for the IOT. They are a network of small, wireless, ad hoc sensor nodes also called motes, which are interconnected and deployed in an area of interest (e.g. home, forest, battlefield, etc.) [1,2]. They are used in a wide range of application scenarios, like military, healthcare, environment, home, etc. [3–10]. The sensor nodes are resource constrained and thus have a limited processing power, transmission range and battery life [2,11–13]. The main purpose of a WSN is the exploitation of multiple

[*] Corresponding author. Tel.: +386 2 2207361; fax: +386 2 2207272.
E-mail addresses: sabzinejad@tmu.ac.ir (M.S. Farash), muhamed.turkanovic@gmail.com (M. Turkanović), saryusiirohi@gmail.com (S. Kumari), marko.holbl@um.si (M. Hölbl).

http://dx.doi.org/10.1016/j.adhoc.2015.05.014
1570-8705/© 2015 Elsevier B.V. All rights reserved.

and interconnected sensor nodes which are deployed in an area of interest where they are sensing the environment and transmit the sensed data to the end user. Similar to this, the idea of the IOT is that everything (e.g. machines, appliances, computers, humans, etc.) is accessible, sensed and interconnected through the wide structure of internet [14].

Since WSNs are evermore attached to the IOT phenomenon, they present new challenges and opportunities. An example of such was presented by Turkanović et al.'s [15], where they outline the problem of a user (i.e. part of the IOT) who wants to connect to a single sensor node from a WSN. A considerable amount of user authentication schemes for WSN were presented in the literature, whereby the vast majority of those applies the principle where a user first connects to the gateway node in order to access the data from the WSN or a single sensor node [16–21]. Turkanović et al. argued and presented a novel scheme where a random user can try and connect to a single sensor node from the WSN. The user gets access to the data gathered by the node if he/she successfully passes the user authentication and key agreement scheme, thus the user has to be registered with the network. The scheme enables any user to register, whereby all the necessary credentials for a successful authentication are safely saved to the smart card. The authentication process is run over the gateway node but the user never interacts with it directly, since this is done by the chosen sensor node.

Turkanović et al.'s scheme is lightweight and resource friendly since it uses only hash and XOR computations (i.e. symmetric cryptography), which is highly desirable by the resource constrained architecture of the WSN. Furthermore the scheme provides mutual authentication between all parties, password protection, free password choice, password changing and dynamic node addition. Unfortunately, although the authors claim resilience to a vast list of cryptographic attacks, we have found that Turkanović et al.'s scheme suffers from smart card stolen attack and man-in-the-middle attack. Moreover, the scheme does not provide untraceability and forward/backward secrecy.

In this paper we aim to identify and present the vulnerabilities and the shortcomings of Turkanović et al.'s scheme [15] (i.e. smart card stolen attack, man-in-the-middle attack, untraceability and forward/backward secrecy). Furthermore in order to overcome the vulnerabilities we propose an improved user authentication and key agreement scheme for HWSN. As we will show later in the security and performance analysis, our new scheme has a higher security level and is still highly efficient. In order to prove the security of our scheme we conducted an analysis with BAN-logic and AVISPA tools.

The remainder of the paper is organized as follows. Section 2 presents an overview of some related work in this field. Section 3 provides a brief review of Turkanović et al.'s scheme, whereby the problems and the shortcomings of the reviewed scheme are presented in Section 4. Section 5 presents our new proposed scheme which removes the shortcomings and improves the scheme of Turkanović et al.'s. We present the analysis of the proposed scheme in Section 6. Finally we conclude the paper in Section 7.

2. Related works

In recent years the science community has focused on the security of WSN. Because of the resource constrained environment of the WSN, classic security mechanisms cannot be applied since they consume too much energy, hence researches are proposing new lightweight security mechanisms for every possible security aspect of WSN (e.g. secure and efficient routing protocols, secure data aggregation, intrusion detection, etc.) [22–26]. This section focuses on the user authentication and key agreement security aspect and presents some cryptographic schemes related to Turkanović et al.'s.

In 2006 Wong et al. proposed a lightweight user authentication scheme for WSN based only on hash and XOR computations [27]. The symmetric scheme was highly promising since it was less complex and designed for resource constrained environment like the WSN. Unfortunately the scheme was proved vulnerable to multiple attacks and thus unappropriated for use. In 2009 Das et al. used Wong et al.'s scheme as the basis for their scheme [28]. They managed to enhance and improve Wong et al.'s scheme by adding a third party to the authentication process, i.e. they added the gateway node (GWN). Their scheme exploits the fact that *GWN* are more powerful than ordinary sensor nodes and thus can transfer the extra computations required onto the *GWN* [2]. The scheme was still lightweight but was later on proved to have some drawbacks and flaws (e.g. does not provide key agreement). After that several authors proposed improvements of Das et al.'s scheme but their schemes were still not efficient as first thought [18,29,30]. In 2010 Khan and Alghathbar also presented a scheme based on Das et al.'s [31]. They presented several improvements of Das et al.'s scheme by introducing password hash values and mutual authentication between the *GWN* and the sensor nodes by using preshared keys. A similar attempt was also presented by Chen and Shih but their scheme was later shown as vulnerable to replay, forgery and bypassing attacks [32]. Moreover Khan and Alghathbar's scheme was also proven insecure by Vaidya et al. [33]. Most recently Das et al. presented a user authentication schemes which encompasses the power of smart cards [34]. The scheme provides mutual authentication between all parties involved in the key agreement, resilience against several attacks and enables a dynamic node addition. The scheme uses only hash and XOR computation and it is thus appropriate for resource constrained environments like WSN. Unfortunately Das et al.'s scheme was later proven to be infeasible for implementations, due to some design flaws and vulnerability to some attacks [17,35–37]. Also recently Xue et al. presented an efficient and lightweight user authentication and key agreement scheme based on temporal credentials [16]. The scheme gathered a lot of attention but was later on proved insecure and vulnerable [36,38,39]. A brief overview of the history of privacy-preserving two-factor authentication schemes can be found in [38].

Meanwhile other researches proposed asymmetric-based cryptographic schemes for authentication and key agreement for WSN. In 2009 and 2010 Xu et al. and Song proposed the use of asymmetric-based schemes for the WSN, while in 2011 Yeh et al. proposed the first ECC-based scheme for WSN [20,40,41]. The problem with these schemes was the memory